Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity Issues and Challenges: In Brief

Eric A. Fischer
Senior Specialist in Science and Technology

December 16, 2014

Congressional Research Service
7-5700
www.crs.gov
R43831

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The information and communications technology (ICT) industry has evolved greatly over the last half century. The technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others. Over the past several years, experts and policy makers have expressed increasing concerns about protecting ICT systems from cyberattacks, which many experts expect to increase in frequency and severity over the next several years.

The act of protecting ICT systems and their contents has come to be known as cybersecurity. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It is also sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. However, cybersecurity can be an important tool in protecting privacy and preventing unauthorized surveillance, and information sharing and intelligence gathering can be useful tools for effecting cybersecurity.

The management of risk to information systems is considered fundamental to effective cybersecurity. The risks associated with any attack depend on three factors: threats (who is attacking), vulnerabilities (how they are attacking), and impacts (what the attack does). Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities, and lessening impacts.

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. On average, federal agencies spend more than 10% of their annual ICT budgets on cybersecurity.

More than 50 statutes address various aspects of cybersecurity, and new legislation has been debated since at least the 111th Congress. Executive Order 13636 and Presidential Policy Directive 21, released in February 2013, address the cybersecurity of CI through voluntary public/private sector collaboration and use of existing regulatory authorities. Four bills enacted in December 2014 address the security of federal ICT, the cybersecurity workforce at the Department of Homeland Security (DHS), and DHS information-sharing activities. Other bills would address information sharing more broadly, research and development, protection of CI, notification of victims of data breaches, and cybercrime laws, among other issues.

The executive-branch actions and proposed legislation are largely designed to address several well-established near-term needs in cybersecurity. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment. Legislation and executive actions in the 114th Congress could have significant impacts on those challenges.

Contents

The Concept of Cybersecurity 1
Management of Cybersecurity Risks 2
What Are the Threats? 2
What Are the Vulnerabilities? 2
What Are the Impacts? 2
Federal Role 3
Executive Order 13636 3
Legislative Proposals 5
Long-Term Challenges 6

Figures

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles 4

Tables

Table 1. Federal FISMA and IT Spending 5

Contacts

Author Contact Information 7

The information technology (IT) industry has evolved greatly over the last half century. Continued, exponential progress in processing power and memory capacity has made IT hardware not only faster, but also smaller, light, cheaper, and easier to use.

The original IT industry has also increasingly converged with the communications industry into a combined sector commonly called information and communications technology (ICT). This technology is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others.

The Concept of Cybersecurity

Over the past several years, experts and policy makers have expressed increasing concerns about protecting ICT systems from *cyberattacks*—deliberate attempts by unauthorized persons to access ICT systems, usually with the goal of theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years.[1]

The act of protecting ICT systems and their contents has come to be known as *cybersecurity*. A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:

- A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace.[2]
- The state or quality of being protected from such threats.
- The broad field of endeavor aimed at implementing and improving those activities and quality.[3]

It is related to but not generally regarded as identical to the concept of *information security*, which is defined in federal law (44 U.S.C. §3542(b)(1)) as

> protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide-
>
> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
>
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
>
> (C) availability, which means ensuring timely and reliable access to and use of information.

[1] See, for example, Lee Rainie, Janna Anderson, and Jennifer Connolly, *Cyber Attacks Likely to Increase* (Pew Research Internet Project, October 2014), http://www.pewInternet.org/2014/10/29/cyber-attacks-likely-to-increase/.

[2] The term *cyberspace* usually refers to the worldwide collection of connected ICT components, the information that is stored in and flows through those components, and the ways that information is structured and processed.

[3] For a more in-depth discussion of this concept, see CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer.

Cybersecurity is also sometimes conflated inappropriately in public discussion with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. Privacy is associated with the ability of an individual person to control access by others to information about that person. Thus, good cybersecurity can help protect privacy in an electronic environment, but information that is shared to assist in cybersecurity efforts might sometimes contain personal information that at least some observers would regard as private. Cybersecurity can be a means of protecting against undesired surveillance of and gathering of intelligence from an information system. However, when aimed at potential sources of cyberattacks, such activities can also be useful to help effect cybersecurity. In addition, surveillance in the form of monitoring of information flow within a system can be an important component of cybersecurity.[4]

Management of Cybersecurity Risks

The risks associated with any attack depend on three factors: *threats* (who is attacking), *vulnerabilities* (how they are attacking), and *impacts* (what the attack does). The management of risk to information systems is considered fundamental to effective cybersecurity.[5]

What Are the Threats?

People who perform cyberattacks generally fall into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing classified or proprietary information used by government or private entities; *nation-state warriors* who develop capabilities and undertake cyberattacks in support of a country's strategic objectives; "*hacktivists*" who perform cyberattacks for nonmonetary reasons; and *terrorists* who engage in cyberattacks as a form of non-state or state-sponsored warfare.

What Are the Vulnerabilities?

Cybersecurity is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix.

What Are the Impacts?

A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. *Cybertheft* or *cyberespionage* can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without

[4] See, for example, Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," June 24, 2014, http://www.dhs.gov/cdm.

[5] See, for example, National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

the knowledge of the victim. *Denial-of-service* attacks can slow or prevent legitimate users from accessing a system. *Botnet* malware can give an attacker command of a system for use in cyberattacks on other systems. Attacks on *industrial control systems* can result in the destruction of the equipment they control, such as generators, pumps, and centrifuges.

Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.

Reducing the risks from cyberattacks usually involves (1) removing the threat source (e.g., by closing down botnets or reducing incentives for cybercriminals); (2) addressing vulnerabilities by hardening ICT assets (e.g., by patching software and training employees); and (3) lessening impacts by mitigating damage and restoring functions (e.g., by having back-up resources available for continuity of operations in response to an attack).

Federal Role

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal systems. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity, and new legislation has been debated since at least the 111th Congress. However, until the end of the 113th Congress, no bills on cybersecurity had been enacted since the Federal Information Security Management Act (FISMA) in 2002.

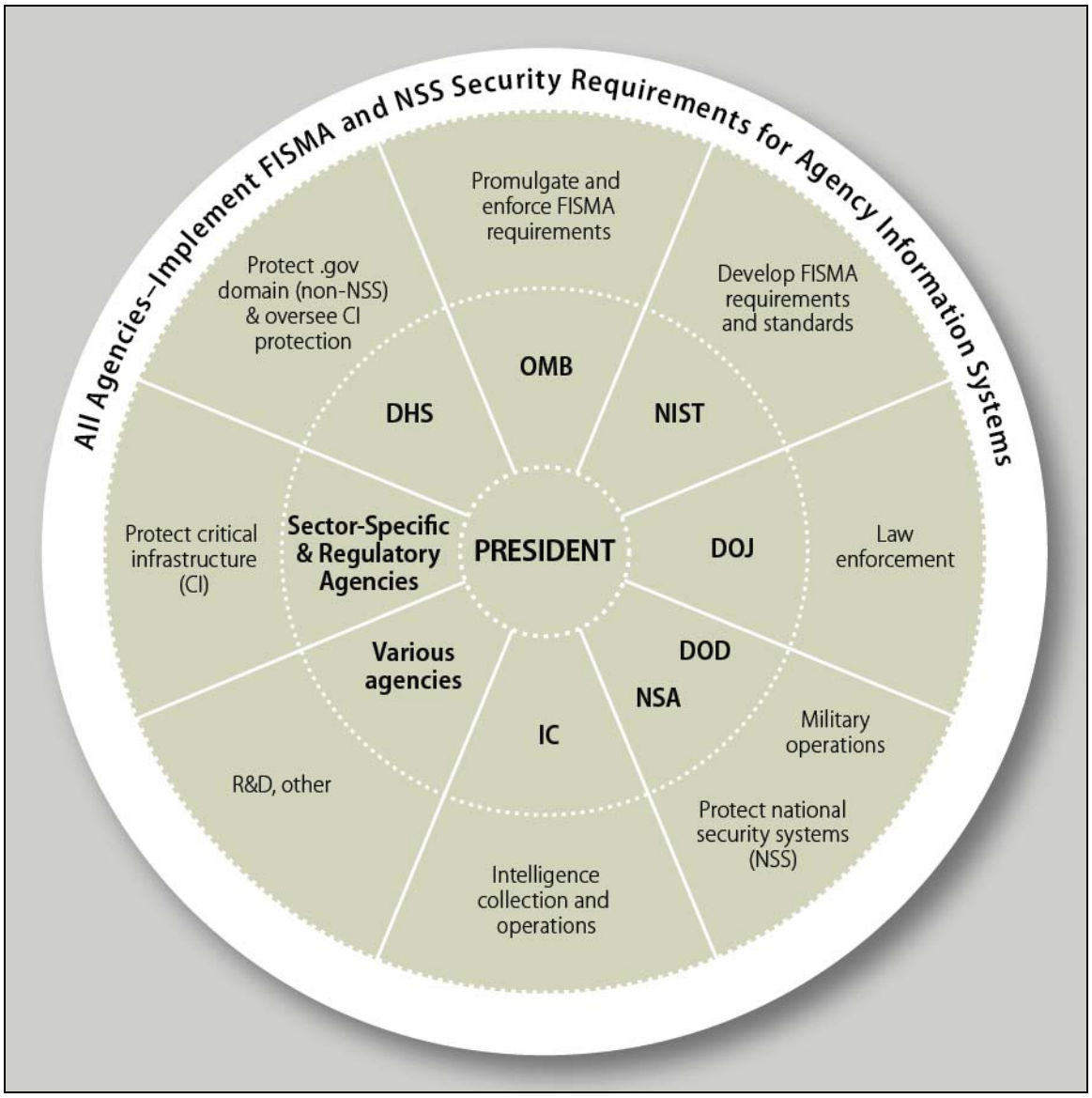
Figure 1 is a simplified schematic diagram of major agency responsibilities in cybersecurity. In general, the National Institute of Standards and Technology (NIST) develops FISMA standards that apply to federal civilian ICT, and the Office of Management and Budget (OMB) is responsible for overseeing their implementation. The Department of Defense (DOD) is responsible for military cyberdefense and, through the National Security Agency (NSA), security of national security systems (NSS), which handle classified information. NSA is also part of the Intelligence Community (IC). The Department of Homeland Security (DHS) has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting CI assets under their control. The Department of Justice (DOJ) is the lead agency for enforcement of relevant laws.

Executive Order 13636

In February 2013, the White House issued Executive Order 13636 and Presidential Policy Directive 21 to address CI cybersecurity through voluntary public/private sector collaboration and use of existing regulatory authorities. Among other things, the documents expanded an existing DHS information-sharing program and required NIST to lead public/private development of a Cybersecurity Framework of standards and best practices for protecting CI. Released in February 2014, the Framework received positive reviews, but it appears too early to determine the extent to which it will improve CI cybersecurity. For more information, see CRS Report R42984, *The 2013*

Cybersecurity Executive Order: Overview and Considerations for Congress, by Eric A. Fischer et al.

Figure 1. Simplified Schematic Diagram of Federal Agency Cybersecurity Roles



Source: CRS

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; OMB: Office of Management and Budget; R&D: Research and development.

Federal agencies spend a significant part of their annual IT funding on cybersecurity, which currently constitutes more than one in every eight dollars of agency IT budgets (**Table 1**).

Legislative Proposals

Since the 111th Congress, many bills have been introduced that would address cybersecurity issues. The main issues addressed by the bills are

- **Information Sharing**—easing access of the private sector to classified threat information and removing barriers to sharing within the private sector and with the federal government. *Controversies:* Roles of DHS and the IC, impacts on privacy and civil liberties, and risks of misuse by the federal government or the private sector.
- **FISMA Reform**—updating the 2002 law to reflect changes in ICT and the threat landscape. *Controversies:* Role of DHS, OMB, and Commerce, and flexibility of requirements.
- **R&D**—updating agency authorizations and strategic planning requirements. *Controversies:* Agency roles, topics for R&D, and levels of funding.
- **Workforce**—improving the size, skills, and preparation of the federal and private-sector cybersecurity workforce. *Controversies:* Hiring and retention authorities, occupational classification, recruitment priorities, and roles of DHS, NSA, the National Science Foundation (NSF), and NIST.
- **Privately Held CI**—improving protection of private-sector CI from attacks with major impacts. *Controversies:* Roles of DHS and other federal agencies, and regulatory vs. voluntary approach.
- **Data-Breach Notification**—requiring notification to victims and other responses after data breaches involving personal or financial information of individuals. *Controversies:* Federal vs. state roles and what responses should be required.
- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity. *Controversies:* Adequacy of current penalties and authorities, impacts on privacy and civil liberties.

Four bills—on FISMA reform (S. 2521), the DHS cybersecurity workforce (H.R. 2952 and S. 1691), and a DHS information sharing center (S. 2519)—were enacted in December 2014. For more information, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation*, by Eric A. Fischer.

Table 1. Federal FISMA and IT Spending

Billions of Dollars, FY2006 to FY2013

Fiscal Year	2006	2007	2008	2009	2010	2011	2012	2013
FISMA Spending	5.5	5.9	6.2	6.8	12.0	13.3	14.6	10.3
Total IT Spending	66.2	68.2	72.8	76.1	80.7	76.0	75.0	73.2
FISMA Proportion of Total IT Spending (%)	*8.3*	*8.7*	*8.5*	*8.9*	*14.9*	*17.5*	*19.5*	*13.8*

Source: Data on FISMA spending are from annual reports on implementation of FISMA from the Office of Management and Budget (OMB), many of which are available at http://www.whitehouse.gov/omb/e-gov/docs. Data on total IT spending are from OMB Exhibit 53 spreadsheets (see Office of Management and Budget,

"Exhibit 53 Archive," Federal IT Dashboard, August 31, 2014, https://itdashboard.gov/exhibit53report for recent documents).

Notes: FISMA data for FY2006-FY2009 are not comparable to later data, and data from 2013 are not comparable to earlier data, because of changes in how OMB collected the information. Amounts for both FISMA and IT spending are reported in the documents as "actual" expenditures and therefore probably consist mostly of obligated funds. Federal documents provide data as IT, not ICT, spending, but include investments in activities such as telecommunications (Office of Management and Budget, "Guidance on Exhibit 53—Information Technology and E-Government," August 5, 2011, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy13_guidance_for_exhibit_53-a-b_20110805.pdf).

Long-Term Challenges

The executive-branch actions and proposed legislation are largely designed to address several well-established near-term needs in cybersecurity: preventing cyber-based disasters and espionage, reducing impacts of successful attacks, improving inter- and intrasector collaboration, clarifying federal agency roles and responsibilities, and fighting cybercrime. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment (DICE):

Design: Experts often say that effective security needs to be an integral part of ICT design. Yet, developers have traditionally focused more on features than security, for economic reasons. Also, many future security needs cannot be predicted, posing a difficult challenge for designers.

Incentives: The structure of economic incentives for cybersecurity has been called distorted or even perverse. Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure.

Consensus: Cybersecurity means different things to different stakeholders, with little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations.

Environment: Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics.

Legislation and executive actions in the 114th Congress could have significant impacts on those challenges. For example, cybersecurity R&D may affect the design of ICT, cybercrime penalties may influence the structure of incentives, the Framework may improve consensus about cybersecurity, and federal initiatives in cloud computing and other new components of cyberspace may help shape the evolution of cybersecurity.

Author Contact Information

Eric A. Fischer
Senior Specialist in Science and Technology
efischer@crs.loc.gov, 7-7071